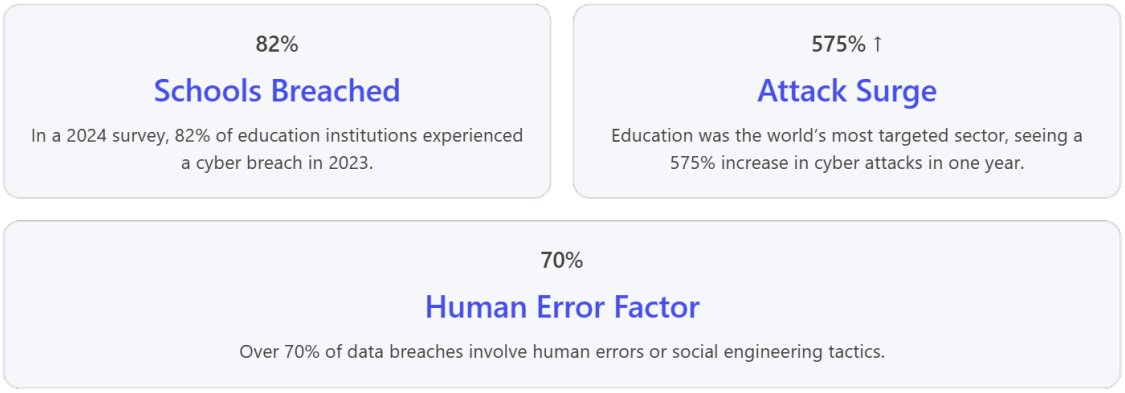
Creating a Cyber Aware Culture in Ontario's K-12 School Boards

Cyber threats are **no longer an IT-only issue – they affect every level of our education system**. Recent incidents across Canada's schools have underscored this reality. In one Ontario district, students returned from winter break to find no internet access and disrupted communications due to a cyberattack [1]. In another case, a teacher uncovered that *17 staff members* had unwittingly surrendered their passwords in a phishing scam [2]. These examples drive home a clear message: **building a cyber aware culture is now essential** to protect our students, staff, and school communities. This article explains what a "cyber aware culture" means in a K-12 context, why it's critical, the benefits it brings, the risks of ignoring it, and how senior leaders can implement and sustain such a culture.



These numbers highlight both the **scale of the threat** and the **opportunity**: if human behavior is a factor in most incidents, then improving awareness and practices can dramatically reduce risks. As one cybersecurity expert put it, *"cybersecurity is a team sport"* – everyone must play a part in defense [1]. A cyber aware culture makes that possible.

What is a Cyber Aware Culture in K-12?

A cyber aware culture means that every member of the school board community is mindful of cyber risks and plays an active role in safeguarding information. In a K-12 school board, this culture extends from the board office to the classroom: trustees, directors, superintendents, IT staff, teachers, students, and even parents share a common understanding of cybersecurity basics and best practices. It's an

---

[1] Cyberattacks can take entire school networks out. It's time to pay more ...

[2] National approach to cyber security education needed as attacks will ...

environment where **people are trained to avoid, recognize, and report cybersecurity threats** – rather than leaving everything to the IT department [3].

Key components of a cyber aware culture include:

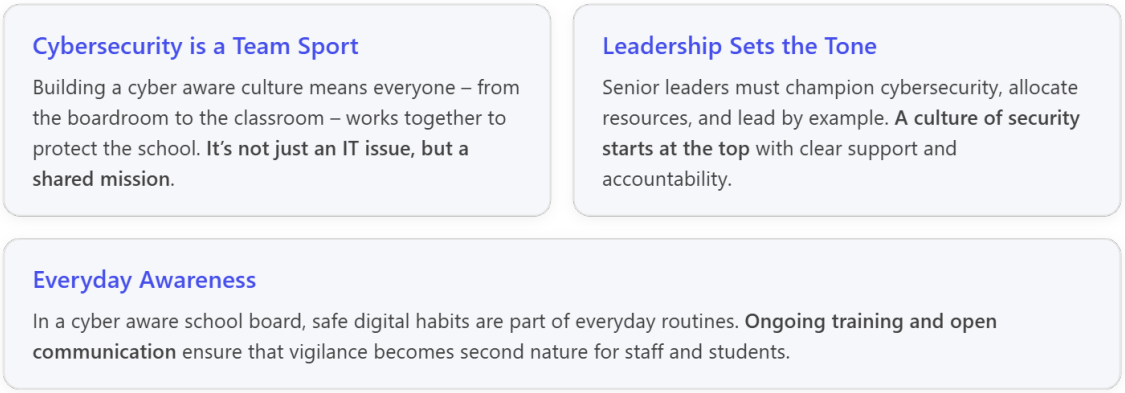
- **Shared Responsibility:** Security is *"everyone's responsibility"*, though it is led and supported by senior leadership [3]. **All levels – from administrative offices to students – are engaged.** In fact, Ontario's education guidelines emphasize creating a cybersecurity and privacy awareness culture *"across all schools, the school board and at all levels of the organization"* to significantly reduce the risk of breaches [4].
- **Leadership and Accountability: Leadership sets the tone.** The commitment of senior management is critical to success [3]. Board leaders must champion cybersecurity in strategic plans, allocate resources, and enforce policies. They also ensure compliance with regulatory requirements and internal policies – a core duty of leadership in protecting privacy [5]. When top leaders visibly prioritize cybersecurity (for example, making it a standing item in meetings and communications), it signals its importance throughout the organization.
- **Continuous Education: Ongoing training and awareness** activities are the backbone of the culture. Staff and students receive regular education on how to spot phishing emails, use strong passwords, safeguard data, and practice safe online behavior. The goal is to ingrain safe habits so that cautious, security-conscious behavior becomes second nature in daily work and learning. Everyone should know how to "stop and think" before clicking suspicious links or sharing sensitive info. For example, teacher Timothy King advises staff to *"just stop – be suspicious"* when something unexpected appears, reinforcing a cautious mindset [2].
- **Open Communication:** In a cyber aware culture, communication about threats and incidents is **transparent and non-punitive**. People are encouraged to report cybersecurity concerns or mistakes (like clicking a bad link) immediately, without fear of blame, so that rapid response can occur. Lessons learned from incidents are shared to prevent future mistakes. This openness helps eliminate stigma around cybersecurity and treats it as a learning opportunity for all.
- **Integration into Daily Activities:** Cyber awareness isn't limited to annual training modules – it's woven into daily school life. Teachers incorporate digital safety into lessons; IT teams routinely share "security tips of the week";

[3] Creating a culture of cybersecurity in your business

[4] Cyber Security and Privacy Awareness - cpco.on.ca

[5] ECNO Announces New Director of Security Services - ECNO

principals discuss online safety in school assemblies. Security practices (like identity verification for sensitive requests or double-checking unusual emails) are built into standard operating procedures. Over time, these practices become as routine as locking the school doors at night.



In practice, a cyber aware culture in K-12 creates a safer, more resilient educational environment. People understand why cybersecurity matters for education, know their role in protecting data and systems, and feel empowered to act securely. The result is not only stronger defenses against cyber threats, but also a community that values and protects privacy, safety, and learning continuity.

Benefits for the School Board

Embracing a cyber aware culture yields significant benefits for the school board organization itself, especially at the leadership and operational level:

- **Reduced Risk of Breaches and Disruptions:** The foremost benefit is lower likelihood of costly cyber incidents. When staff and students are vigilant (e.g. recognizing phishing attempts and using secure practices), the "human error" factor in breaches drops dramatically. This can *"significantly reduce the risk of cybersecurity and data breaches"* across the board [4]. Fewer incidents mean less downtime for IT systems and minimal disruption to classroom instruction. Keeping school networks up and running is critical – a successful cyberattack can otherwise *"derail day-to-day operations in every single school"* by knocking out networks and data access [1]. A cyber aware culture helps prevent such worst-case scenarios.
- **Protection of Sensitive Data & Privacy Compliance:** School boards hold a **vast trove of personal information** on students, families, and staff – making privacy a top concern. A strong security culture helps safeguard this data from unauthorized access or leaks. This is not just good practice but also a legal and ethical mandate. Ontario's privacy laws (MFIPPA) require boards to protect

personal information, and new provincial standards are raising the bar even further. In 2025, Ontario introduced an explicit requirement for public institutions to *"take reasonable steps to protect personal information… against theft, loss and unauthorized use or disclosure"* [6]. **Cultivating cyber awareness ensures everyone follows protocols that keep student records and personal data safe**, thereby keeping the board in line with regulatory requirements and maintaining public trust [6]. Avoiding privacy breaches also means avoiding potential penalties and compliance issues.

- **Financial Safeguard and Cost Avoidance:** Breaches can be extremely expensive – recovering systems, paying cyber incident response costs, potential ransom payments, notifying affected individuals, and dealing with legal fallout all carry high costs. A proactive cybersecurity culture is far cheaper than reacting to a major incident. By preventing incidents (or minimizing their impact), boards avoid the **hefty financial losses** associated with cyberattacks. Additionally, cyber awareness can lead to reduced insurance premiums or better terms, as insurers recognize the lower risk.
- **Operational Continuity and Resilience:** Building cyber awareness improves the board's resilience. Staff are prepared to respond calmly and correctly if something suspicious occurs, following established procedures. Important services like online learning platforms, email, and attendance systems are less likely to be taken down for long periods. This ensures **teaching and learning can continue with minimal interruption, even in the face of cyber threats**. For example, having an incident response plan and an informed team means that even if an attack happens, it's contained and resolved faster [1]. In short, a cyber aware board can "take a punch" and get back on its feet quickly, which is crucial for delivering education without prolonged outages.
- **Reputation and Community Trust:** Parents and the wider community expect the school board to protect student information and provide safe learning environments. Demonstrating strong cybersecurity practices bolsters trust. Conversely, a serious data breach can **erode public confidence** – families may worry about identity theft, or question the board's competency. Senior leaders, especially Directors of Education and Superintendents, are keenly aware of their duty as stewards of student data. By investing in cybersecurity culture, boards show accountability and care, reinforcing their reputation as responsible guardians of students' well-being. *Maintaining that trust* is paramount in the education sector [6].
- **Empowered Innovation:** When a board has appropriate security measures ingrained in its culture, it actually **frees the organization to innovate with**

[6] Bill 194, the Strengthening Cyber Security and Building Trust in the …

confidence. Leaders can pursue new digital learning tools and cloud services knowing that risk is being managed. For instance, one Ontario board's strong leadership in IT and security enabled it to become a leader in adopting cloud technologies safely [5]. Staff who are cyber-aware can embrace technology (like online collaboration platforms or e-learning apps) without as much fear, because they know how to use them securely. Thus, a cyber aware culture can be an enabler for educational innovation rather than a barrier.

In summary, a cyber aware culture acts as an **insurance policy and a performance booster** for the school board: protecting against disasters while enhancing day-to-day reliability and stakeholder confidence. It aligns cybersecurity with the board's overall mission – ensuring safe, uninterrupted education.

Benefits for Staff, Students, and the Community

A culture of cybersecurity doesn't just benefit the organization; it brings **tangible advantages to all stakeholders** in the school board community – including staff members, students, parents, and the broader community. Here's how:

For Staff and Educators: Teachers, principals, and support staff gain peace of mind and valuable skills. In a cyber aware environment, staff are less likely to fall victim to scams that could compromise their personal information or the school's systems. They learn to **recognize threats like phishing emails and handle them confidently** (for example, verifying any unusual request that might be a scam). This reduces personal stress (no one wants to be the person who accidentally opened the door to an attacker) and creates a more positive, empowered work culture. Moreover, cybersecurity training contributes to professional development – staff improve their digital literacy and stay current with technology. Given that *"IT underlies everything"* in modern education [2], being savvy about cyber safety is now a core competency for educators. Staff also feel supported knowing the board has their back with clear procedures if something does go wrong (e.g. who to call if they suspect a breach). Overall, employees are safer and more confident in using technology for teaching and administration.

For Students: A cyber aware culture directly translates into a **safer learning environment and crucial life lessons** for students. Today's students are growing up immersed in technology; by embedding cybersecurity awareness in school culture, we help them develop healthy online habits and critical thinking skills. They learn how to protect their privacy, handle cyberbullying or suspicious messages, and become responsible digital citizens. These lessons extend beyond IT class – they are reinforced through campaigns, assemblies, and curriculum integration. Ontario's school system, for instance, provides resources like the *Cyber Security Ontario K-12 "Zone"* with games and videos *"designed to help our future generations stay protected as they grow*

up in our ever-evolving digital world" [2]. *Students benefit* from fewer disruptions too: when schools avoid major IT outages due to ransomware or other attacks, students don't lose valuable class time or access to learning materials. Additionally, engaging students in cybersecurity (through clubs, challenges, or coursework) can spark interest in STEM and cybersecurity careers – a field in high demand. In short, students not only gain protection but also education: **they acquire knowledge and skills that will serve them for life** in a digital society.

For Parents and Families: Parents entrust school boards with their children's personal data and safety. A strong cybersecurity culture provides **reassurance to families** that this trust is well placed. It means the board is taking concrete steps to keep parent and student information (addresses, health info, report cards, etc.) secure from identity thieves or hackers. This reduces the anxiety of receiving those "dreaded notices" about data breaches in the school system [1]. Instead, parents can be confident that privacy is respected and protected. Furthermore, a cyber aware culture often includes **parent outreach and education**. Boards may share tips with parents on safe online practices for kids at home or alert families promptly about any emerging cyber threats targeting students. This partnership helps parents reinforce the same safe habits at home, creating a consistent message for children. For example, if a phishing scam impersonates the school, a cyber-savvy parent who has been educated by school communications will know how to verify it and not be duped. Ultimately, families experience *greater trust and satisfaction* with the school board when they know cybersecurity is a priority.

For the Community and Society: Beyond the immediate school community, there are broader societal benefits. K-12 schools are part of our critical infrastructure – keeping them secure helps protect our local communities from disruption. A ransomware attack on a school board can have ripple effects (for instance, if schools close or if personal data is stolen for fraud in the community). By building resilience against such attacks, boards contribute to the stability of the community. Additionally, **fostering cyber awareness in youth has long-term social benefits**: students carry their knowledge into post-secondary education and the workforce, meaning tomorrow's citizens and employees are more cyber literate. This helps raise the overall cybersecurity posture of our society over time. School boards that promote cybersecurity also often share knowledge with other local institutions (libraries, community centers) and lead by example in the public sector. All of this fortifies the community's overall defense against cyber threats. As Ontario's Minister of Public and Business Service Delivery noted, we must teach cyber safety to youth because the province is increasingly digital and we need everyone to practice strong security to protect data and services [2]. A cyber aware school board is a community leader in that effort.

In summary, **every stakeholder gains when a cyber aware culture is in place**. Staff and students are safer and more informed. Parents have greater peace of mind. The community enjoys more reliable education services and a generation better prepared for the digital world. These human-centric benefits are a powerful complement to the organizational benefits – together they make the case that cybersecurity culture is not just an IT initiative, but a holistic improvement for the entire school ecosystem.

Risks of Not Creating a Cyber Aware Culture

What happens if a school board does **not** foster a cyber aware culture? The risks are serious and increasingly untenable in today's threat landscape. Without a culture of cybersecurity, a board is essentially **leaving its front door unlocked** for attackers. Key risks include:

- **High Likelihood of Cyber Incidents:** In the absence of awareness, it's not a question of *if* a cyber incident will occur, but *when*. Attackers actively target the education sector – drawn by rich data stores and sometimes outdated defenses. Schools have become *"attractive targets"* for cybercriminals [1]. If staff and students are not educated on threats, the board is far more vulnerable to common attacks like phishing, malware infections, or ransomware. One unwitting click on a malicious email can lead to an entire network of schools being compromised. Consider the example of a teacher phishing scenario: 17 employees handed over their credentials before one tech-savvy teacher intervened [2]. Without that intervention or prior training, that incident could have escalated into a full-blown breach of the board's systems. **Lack of cyber awareness dramatically raises the probability of successful attacks**, as attackers will exploit the human factor. Given that over 70% of breaches involve human error or social engineering [4], not addressing that human factor is a recipe for disaster.
- **Severe Disruption to Education:** A major cyber incident can **bring school operations to a halt** if a board isn't prepared. For instance, a ransomware attack might encrypt critical data and knock out systems needed for everything from taking attendance to contacting parents. We've seen cases where an entire school division had "basically everything we use" go down – computers, PA systems, the internet – for weeks [1]. Without a culture of preparedness (where everyone knows what to do and how to prevent spread), recovery can be slow and chaotic. This means lost instructional days, cancelled classes, inability to access learning resources, and general turmoil. Important safety functions (like emergency communication systems) could fail when needed [1]. **The risk of not**

being cyber aware is essentially risking the ability to carry out the board's educational mission.

- **Compromise of Sensitive Data:** School boards hold decades of sensitive data – academic records, personal identities, even health and special education information. A lapse in cybersecurity can lead to massive data breaches. Recently, a breach of a common school software platform exposed student and staff data going back decades, even including things like social insurance numbers in some cases [7]. Without a strong culture of security, such breaches may go undetected longer and end up more extensive. The fallout can be severe: exposed individuals face identity theft risks (criminals can use a student's identity to open fraudulent accounts [1]), and the board faces legal liabilities and costs. Privacy commissioners would investigate, and the board could be found negligent if basic protections and awareness weren't in place. **Not cultivating cyber awareness puts students' and employees' privacy in peril**, which can erode trust for years to come.
- **Financial and Legal Consequences:** The cost of a cyber incident can be enormous, especially if the board must respond from scratch. There may be ransom payments demanded by attackers who lock up data; even if not paid, technical recovery can cost hundreds of thousands of dollars in IT overtime, equipment, and external experts. Without awareness, staff might also be more likely to violate regulations (for example, mishandling student data or not reporting an incident promptly), which can result in legal penalties. With new legislation emerging, boards that don't follow cybersecurity best practices could face stricter scrutiny. For instance, while Ontario's new **Bill 194** mandates breach reporting and protection for provincial agencies [6], school boards are expected to adopt similar best practices to *"reduce risk… and maintain public trust"* [6]. A board that neglects cyber awareness could find itself on the wrong side of compliance if (or when) these expectations become enforceable rules. Even in the absence of fines, consider the financial hit of losing donor or government trust after a major breach. Insurers may also raise premiums or refuse coverage to boards with poor security culture, adding further cost.
- **Erosion of Stakeholder Trust:** Perhaps the most irreparable damage from not having a cyber aware culture is the **loss of trust among students, parents, and staff**. Modern families are very aware of cybersecurity issues – they read headlines about school breaches and they expect transparency and competence. If a board suffers a preventable incident due to employee negligence or lack of training, public confidence can plummet. Parents may become hesitant to share information or use online services provided by the

[7] Cyberattack affecting school boards across Canada may involve decades …

board. Staff morale can also suffer – employees don't want to feel like they're working in an unsafe digital environment, or conversely they dread being scapegoated if something goes wrong. News of a board "failing" to protect data can tarnish its reputation for years. Rebuilding trust post-breach is far harder than maintaining it by proactive measures. **In the education sector, trust and credibility are paramount**, and they are at serious risk without a strong cybersecurity ethos.

In short, ignoring cybersecurity culture is a high-stakes gamble with almost guaranteed negative outcomes. The **threat environment for schools is worsening** – attacks are more frequent (+575% in recent years) and sophisticated [4]. Without a vigilant culture, a board is likely to face more frequent incidents and be ill-prepared to deal with them. The consequences span from immediate operational paralysis to long-term financial and reputational damage. As Ontario's privacy commissioner Patricia Kosseim warns, *"cyberattacks are very prevalent... but there's lots that schools and school boards can do to help reduce the risks and impacts"* [1]. The flip side is, if those things *aren't* done, the risks and impacts will only grow. The message is clear: **the cost of not fostering a cyber aware culture far exceeds the effort required to build one.**

How to Implement a Cyber Aware Culture

Developing a cyber aware culture in a K-12 environment requires a strategic, **multi-faceted approach**. It won't happen overnight – but with consistent effort and leadership support, even boards starting from scratch can make significant progress. Below is a step-by-step process senior leaders can follow to implement a culture of cybersecurity:

1. **Assess the Current State:** Begin with a frank assessment of where your board stands in terms of cybersecurity awareness. You can't improve what you don't measure. Evaluate staff and student awareness levels and identify key gaps. This might include conducting surveys or quizzes to gauge knowledge (e.g. do employees know how to spot a phishing email?), reviewing past incident reports for common causes, and even running simulated phishing tests to see how many users fall for them. Consider bringing in an external cybersecurity team or using services from ECNO for a **security governance review** to pinpoint weaknesses [8]. The goal of this stage is to map out critical risk areas – whether it's low awareness of password best practices, lack of incident response planning, outdated policies, or technical vulnerabilities. By establishing a

[8] Security Solutions - ECNO

baseline, you create a benchmark to measure improvement and target your efforts where they are most needed.

2. **Secure Leadership Commitment and Define Goals: Tone from the top is crucial.** The board's senior leadership (Director of Education, superintendents, CIO, etc.) should openly endorse the cybersecurity initiative. Start by defining what "cyber aware culture" means for your board and get buy-in on clear objectives (for example: 100% of staff to complete cybersecurity training this year; or reducing the number of clicking on phishing emails by X%). Assign executive ownership – often the CIO or a dedicated security lead (like a CISO or Manager of Security Services) will drive the program, but *every* executive should be accountable for supporting it. Leadership must also agree to allocate necessary resources, whether budget for training tools or time in staff schedules for awareness activities [3]. **Establish or update governance structures**: this could mean forming a cybersecurity steering committee or task force that includes representatives from IT, academics, HR, and school administration. Right from the start, integrate cybersecurity goals into the board's strategic plans and policies, showing that it's a priority on par with educational outcomes. Leadership commitment also involves modeling good behavior – e.g., executives themselves taking training, following security policies diligently, and talking about cybersecurity in their meetings and communications. When staff see top leaders championing the cause, it reinforces that this is a long-term, serious effort, not a flavor-of-the-month project.
3. **Update Policies and Procedures:** A culture change needs a framework of policies to support it. Review and update the board's cybersecurity-related policies, procedures, and guidelines to ensure they set clear expectations. This might include acceptable use policies (for staff and students), password management rules, remote work/learning security guidelines, data handling and privacy policies, incident response plans, and vendor security requirements. Ensure that **roles and responsibilities are defined** – for example, policies should spell out that *everyone* (employees, students, even contractors or volunteers) has a role in protecting data [4]. Also incorporate references to these policies in training materials, so people connect the training to real expectations [4]. It's important that policies are not just documents on a shelf: socialize them through workshops or summary sheets so that they become living guidelines. **Align policies with regulatory standards and best practices.** For instance, make sure your data protection practices are in line with privacy laws and emerging standards (like those recommended by Bill 194 for safeguarding information [6]). Develop a clear **incident reporting procedure** (who to call, immediate steps) and communicate it to all staff – this encourages the desired behavior of prompt reporting. By establishing strong policies, you create the

backbone of the cyber aware culture, giving everyone a reference point for what is expected.

4. **Educate and Train Continuously: Education is the heart of creating a cyber aware culture.** Launch a comprehensive cybersecurity awareness training program for all staff – and extend it to students, parents, and trustees as appropriate. Key elements include:
    - **Staff Training:** Provide mandatory cybersecurity training for employees and contractors. This can be in the form of e-learning modules, webinars, or in-person workshops. Cover practical topics like how to detect phishing, safe internet browsing, proper data storage, using multifactor authentication, etc. Use relatable examples from the education context (e.g., "What to do if you get an email that looks like it's from the principal but isn't"). Encourage active participation – quizzes, interactive content, and Q\&A sessions to keep it engaging. Fortunately, there are *free or low-cost resources* available to Canadian school boards. For example, Fortinet has an education-focused Security Awareness Training service **offered at no cost to all K-12 school boards in Canada** [9]. It provides up-to-date modules and even tracks completion, making it easier to deploy regular training. Many boards are taking advantage of such offers to build a "cyber-informed" workforce [9].
    - **Student and Classroom Awareness:** Work cybersecurity topics into the student learning experience. This can start with basic digital citizenship lessons in elementary grades (e.g., keeping personal information private, what is a strong password) and progress to more advanced topics in high school (like understanding social engineering, or even introductory cybersecurity courses/clubs for interested students). The Ministry of Education, ECNO, and partners have created age-appropriate content to help with this. For instance, the **annual K-12 Cyber Awareness Month campaign** each October provides videos, games, and lesson plans tailored for K-12 in Ontario [10]. Teachers can use these resources to spark conversations and activities around cyber safety in class. Other initiatives like ECNO's *Cyber Heroes Unite* themes for different grade levels gamify security topics for kids [11]. By leveraging these, boards don't have to reinvent the wheel – they can integrate existing materials into curriculum and school events.

[9] Security Awareness and Training Service: Education Edition

[10] October is K-12 Cyber Awareness Month - Toronto District School Board

[11] Cyber Awareness Month - Grades K-8 - ECNO

- **Parent and Community Outreach:** Include parents and guardians in your awareness efforts. This might involve sending cybersecurity tips in parent newsletters, holding an information night on online safety for kids, or sharing short tutorials on how to secure home Wi-Fi or recognize scams that target parents (e.g., fake school fee emails). When parents practice good cyber hygiene and reinforce it at home, it complements what students learn at school. Some boards share Government of Canada resources like the *Get Cyber Safe* guide for families [12] [12] to educate the broader community. Creating a page on the board's website with cybersecurity updates and resources can also be helpful.
- **Specialized Training for Key Roles:** Provide extra training for staff in sensitive positions – e.g., finance staff (to prevent CEO fraud scams), HR staff (protecting personal data), IT administrators (advanced security skills), and school office administrators (who often manage student records). Tailoring content for these groups ensures they have the deeper knowledge required for their role.
- **Frequent Refreshers and Reminders:** Don't settle for one-and-done training. **Make awareness an ongoing campaign.** Use monthly security newsletters or tip emails, posters in staff rooms, short videos at staff meetings, and yearly refresher courses to keep cybersecurity top-of-mind. Users tend to forget over time, so regular reinforcement is key. For example, you could highlight a "threat of the month" (like January: phishing, February: safe use of cloud apps, etc.) aligning with the *K-12 Cyber Awareness Calendar* that provides year-round themes [12]. Keep the content fresh and update it to include new threats (e.g., warnings about emerging scams or technologies like AI deepfakes).
- **Engage through Positive Culture:** Where possible, make it fun and engaging. Some boards have introduced friendly *phishing challenges* or gamified quizzes with prizes for schools that perform best. ECNO in partnership with Fair Chance Learning recently ran the **Cyber Champion Challenge** which invited students to create art or projects about cybersecurity, making learning "seriously fun" [13] [13]. You can adapt this idea internally – maybe run a contest for classes to make a cybersecurity poster, or have students produce a short skit or video on online safety. Celebrating Cyber Awareness Month in October with school-wide

[12] Cyber Security - Greater Essex County District School Board

[13] Cyber Champion Challenge

activities is another way to build enthusiasm. The point is to integrate security in a positive way, not just as warnings and rules.

Remember to track participation: ensure all staff complete required training and note who might need follow-up. The board could set a policy that, for instance, *all employees must complete cybersecurity training annually* – and tie compliance to performance reviews or other accountability measures. According to research, 97% of education sector decision-makers believe that more training and awareness helps reduce cyber attacks

[9], highlighting just how crucial this education step is.

1. **Engage and Empower All Stakeholders:** Building on training, work to actively engage every stakeholder group in the cyber aware culture. **Cultivate cybersecurity champions** at various levels – these could be tech-savvy teachers or a "Digital Lead" at each school who can help peers with questions and keep the topic alive locally. Encourage student clubs or "cyber ambassadors" (perhaps students who participate in ICT or STEM clubs) to promote safe online practices among their peers. Some schools hold assemblies led by students on topics like cyberbullying and security, which can be very effective due to peer influence. For staff, consider establishing a forum or working group where representatives from different departments discuss cybersecurity concerns and share ideas to improve (e.g., a monthly meeting of school tech reps or a Teams channel dedicated to cybersecurity tips).

It's also important to **empower people to take action**. Make it clear that every individual's vigilance matters. For example, if an education assistant notices a strange email, that person should feel it's their place to speak up and report it. One way to reinforce this is by positively recognizing those who do report incidents or suggest improvements. A simple shout-out in a staff memo like "Thanks to the teacher who alerted IT to a phishing email last week – quick reporting helped us block it board-wide" can reinforce the desired behavior.

Extend engagement to parents and the community as well. Perhaps host a cybersecurity awareness seminar in partnership with parent councils or local public libraries. Work with your communications team to push out cyber awareness messages on social media or board newsletters that reach the wider public. By making cybersecurity a community conversation, you normalize it as part of school life. (As one expert noted, *"Cybersecurity used to be a boardroom conversation. Now it's a kitchen table conversation."*

[1] – in other words, it should be talked about openly in families, not just in IT offices.)

1. **Implement Technical Measures and Incident Readiness (in Parallel):** While culture is about people and process, don't neglect the technology safeguards that support a cyber secure environment. Ensure the board's IT team is applying up-to-date security measures: firewall and network protections, strong email filters, multifactor authentication for staff logins, regular software updates/patching, secure backups, etc. Many Ontario school boards are leveraging collective services for this – for instance, 66 boards across the province participate in ECNO's Security Operations program to access cybersecurity expertise and tools [8]. A robust technical foundation means users have a safety net; even if someone slips up, controls can catch or limit the damage.

At the same time, develop a clear **Cyber Incident Response Plan** and make sure it's known and practiced. This plan should outline how the board reacts to various incidents (data breach, malware outbreak, etc.), including who is on the response team, how to isolate affected systems, communication protocols (internal and to the public), and how to recover operations. Distribute an easy-to-follow incident reporting flowchart to schools so that any staff member knows what to do and whom to call if they suspect a cyber issue. Conduct **tabletop exercises** or drills to go through the response steps for a hypothetical attack

[8]; involving school leadership in these exercises is a great way to build muscle memory. Practicing response not only improves actual readiness but also reinforces the culture by sending the message that "we take this seriously and are prepared." As Patricia Kosseim suggested, IT teams and board leadership should *run through response plans for practice* – like fire drills for cyber incidents [1].

While this step is more operational, it intersects with culture: when people see strong technical defenses and a practiced plan, it builds confidence and encourages them to uphold their end (reporting issues, following protocols) because they know the organization will respond effectively.

1. **Measure Progress and Adapt:** After initiating these improvements, continuously **measure the impact** and adapt as needed. Use metrics (remember, metrics are key to accountability [3]) to track how your culture change is going. Some useful metrics:
    - Phishing simulation results (e.g., the click rate on test phishing emails should decrease over time as awareness improves).
    - Number of security incidents or near-misses reported by staff (initially, you might see an increase in reporting – a good sign people are engaging; over the long term, actual incidents should decline).
    - Training completion rates and quiz scores.

- Survey feedback from staff and students on their confidence in cybersecurity knowledge (are they more comfortable than before?).
- Audit results or compliance checks on whether policies are being followed (for instance, fewer instances of weak passwords or unencrypted USB usage).

Regularly review these indicators at a leadership level. Celebrate successes, such as a school that had 100% training completion or an incident that was swiftly contained due to an employee's quick action. Address areas that are lagging – if, say, a particular department keeps falling for phishing tests, they might need extra attention or different training methods.

Adapt your strategies based on what you learn. Cyber threats also evolve, so the culture program should evolve too. Perhaps this year phishing is the focus, but next year you find that people are struggling with secure cloud document sharing, so you add training in that area. Always seek feedback: create a channel for staff to suggest ideas or express concerns about cybersecurity processes. Maybe teachers are overwhelmed by too many security emails – you might consolidate communications. Or students might find the content boring – perhaps involve them in creating new materials that resonate better with youth. Keeping the culture initiative dynamic and responsive will prevent it from becoming stale or viewed as a checkbox exercise.

1. **Institutionalize and Sustain:** Finally, aim to **embed cybersecurity into the fabric of the board's operations long-term**. New employee onboarding should include cybersecurity orientation (and even new student orientation, in an age-appropriate way). Include cybersecurity considerations in all projects and decisions – for example, any new software a board adopts must go through a security/privacy review, and any new initiative (like 1:1 devices for students) should have an accompanying awareness plan. Make cybersecurity awareness month an annual tradition, and consider aligning it with periodic policy reviews or updates each year. By institutionalizing these practices, the culture will continue regardless of staff turnover or new leadership.

It's also wise to stay connected with external networks – **collaborate and share best practices with other school boards** and organizations. Many boards share threat information and tips through ECNO and other forums

[1]. Such collaboration can inspire new ideas to keep your program fresh. The landscape will keep changing (think about the rise of remote learning during the pandemic – it introduced new security challenges overnight), so sustaining a cyber aware culture means committing to ongoing learning and improvement. As the years go by, aim to keep security awareness as a *perennial priority*, akin to student safety or equity – something that is just part of "how we do education."

Throughout this implementation process, **visible support and reinforcement from senior board leadership is the linchpin**. When employees and the community consistently see leaders prioritizing cybersecurity – through communication, resources, and actions – the culture shift truly takes hold.

Overcoming Common Challenges

Implementing a cyber aware culture is not without challenges. Education environments have unique constraints, and it's normal to encounter some resistance or difficulties along the way. Here are some common challenges school boards face in this journey, **paired with strategies to address them**:

- **Challenge: "Technology is intimidating."** Many educators or staff outside of IT may feel that cybersecurity is overly technical or scary. As one Ontario teacher observed, *people often "stop listening because they get confused"* when technical jargon is used [2]. **Solution:** Demystify the topic. Start with basic digital literacy and relatable concepts. Avoid jargon in your training; use plain language and real-life school scenarios. Emphasize that one doesn't need to be a tech expert to follow basic practices. Providing hands-on, workshop-style training can help reduce fear – for example, a session where staff literally practice checking if an email is phishing or configure privacy settings on a device. Build confidence gradually. Also, promote a growth mindset: remind everyone that cybersecurity is a skill that can be learned, not an innate talent. By framing it as an extension of existing safety practices (like "stranger danger" but online, or locking the school at day's end but for your computer), it becomes less intimidating. Peer learning can help too: have tech-savvy staff mentor others in a friendly, non-judgmental way.
- **Challenge: Limited Resources and Time.** Schools are stretched thin on budgets and staff time for professional development. It can be hard to justify diverting resources to security awareness amid pressing educational needs. **Solution:** Leverage free and cost-effective resources (like the free training platforms offered to Canadian schools [9], or government-provided materials) to reduce financial burden. Incorporate cyber awareness into existing PD days or staff meetings rather than adding separate sessions – piggyback on scheduled gatherings. Emphasize the *cost of not acting*: share data on how much a breach could cost or how it could disrupt learning, to make the case that an ounce of prevention is worth a pound of cure. Also, start small and scale up – you don't need to do everything at once. If time is a major issue, begin with micro-learning: short 5-10 minute trainings or tips that can be consumed without heavy time investment. Prioritize high-impact topics first (like phishing). By showing early

wins (e.g., a phishing test improvement after a quick training), you build the argument for dedicating more time/resources.

- **Challenge: Complacency or Low Perceived Risk.** In some places, there's an attitude of "we're just a school board, who would target us?" or "we haven't had a big incident yet, so we're probably fine." **Solution:** Fight complacency with awareness of reality. Use real-world examples, especially Canadian ones, to show that school boards *are* being targeted. Share news stories of breaches in other school boards (many have occurred across Canada [7] [1]) or statistics like the 575% increase in education cyber attacks [4]. When people see that peers or neighbouring boards have been hit, it creates a sense of "it could happen here tomorrow." Also consider inviting a guest speaker – perhaps someone from a school that experienced an attack – to speak candidly about the consequences. Hearing a first-hand account can shake people out of denial. Another tactic is to run a surprise simulation (with leadership approval): for example, send a very convincing fake phishing email and then share the results: "X% of us clicked this link – this is exactly how an attacker could get in." This provides a wake-up call and a baseline to improve from. The key is to make the threat tangible and personalize the risk so that stakeholders understand the urgency.
- **Challenge: Diverse Audience (one size doesn't fit all).** A school board's community ranges from young students to veteran teachers to busy parents to tech administrators. Crafting an awareness program that resonates with all ages and roles can be difficult. **Solution: Tailor and differentiate** your approach. Segment your audience and use different communication channels and styles for each group. For students, use engaging, age-appropriate content (cartoons, games, interactive activities) – Ontario's cyber awareness curriculum is designed with this in mind [11]. For teachers, focus on practical classroom and personal tech use scenarios. For administrators, highlight policy and compliance aspects. Translate materials into the languages needed in your community to reach parents of all backgrounds. The board should provide **accessible resources that educators can adapt for their classrooms** [4] – this implies giving teachers flexibility to integrate cyber topics in a way that fits their students (a Grade 2 teacher will approach online safety differently than a Grade 10 teacher). Solicit input: ask representatives from each stakeholder group what content or format would help them most. By customizing the messaging, you ensure each audience finds it relevant rather than tuning out.
- **Challenge: Sustaining Momentum.** It's easy to declare a new initiative, but sustaining enthusiasm and compliance over the long term is hard. Staff might participate actively during Cyber Awareness Month but then forget about it afterwards. New initiatives can fade as other priorities crowd in. **Solution:** Make security a regular drumbeat rather than a one-time chorus. Build it into the

calendar (monthly themes, quarterly drills, annual refreshers as policy). Keep the content fresh – update people on new threats (e.g., "There's a new social media scam trending – here's what to know this week"). Use different mediums: mix emails with posters, intranet banners, maybe a humorous video now and then. Also, **leadership needs to keep talking about it consistently**. If the Director mentions cybersecurity in every town hall and the topic shows up frequently in internal newsletters, it stays on everyone's radar. You can also maintain momentum by reporting progress: for instance, share that "we've increased our phishing detection rate by 30% – great job! Here's our next goal." When people see progress and ongoing commitment, they're more likely to stay engaged. Embedding responsibilities into job roles helps; for example, include a security awareness duty in school principals' performance goals or in teacher professional development plans. Over time, these practices become routine.

- **Challenge: Incident Fatigue or Fear of Reporting.** Sometimes, if minor incidents or suspicious activities happen frequently, staff can either become numb ("another virus alert, whatever…") or they might hide incidents out of fear of blame. **Solution:** Create a healthy reporting culture. Ensure that reporting a mistake (like clicking a bad link) is met with appreciation and response, not punishment. Publicize stories where quick reporting saved the day, to reinforce positive behavior. If people aren't reporting, consider anonymous reporting channels or a "no-fault" policy for self-reporting security errors. As for fatigue, try to filter noise – don't overload everyone with every single security alert; let IT handle the noise in the background. Communicate what's necessary in a concise way. Rotate focus areas so it doesn't feel like spam – one month focus on privacy, another on phishing, etc., to keep interest. By cultivating a supportive atmosphere, you ensure people stay alert but not anxious, and that they act when needed.

Every organization will face a mix of these challenges, and possibly others, but **with creative strategies and sustained leadership support, they can be overcome**. Many Ontario school boards have already navigated these hurdles by sharing resources, tapping into provincial initiatives, and learning from each other's experiences. Recognize that building a cyber aware culture is a change management effort at its core – it involves changing people's behaviors and mindsets. This takes time, patience, and adaptability. But the challenges are surmountable, and the payoff – a secure and thriving educational environment – is well worth it.

Best Practices for Maintaining a Cyber Aware Culture

Once you've established the foundations of a cyber aware culture, the work is not done – it's an ongoing commitment. **Cybersecurity is a constantly evolving field**, so a

successful culture must also evolve and reinforce itself. Here are best practices to keep the momentum and continuously strengthen that culture over time:

- **Keep Training Relevant and Ongoing:** Regularly update your training content to reflect new threats and technologies. Threat actors are always changing tactics, whether it's new phishing themes (e.g. COVID-19 scams one year, cryptocurrency scams the next) or emerging issues like deepfakes. Ensure your awareness program stays current so that staff and students are prepared for *today's* risks, not yesterday's. Refresh training **at least annually** for all staff – many boards do it every year as part of compliance. Ontario's guidance suggests that with ever-evolving threats and tech, training should be **refreshed regularly** [4]. Consider brief mid-year refreshers too, not just one big yearly session. Make sure newcomers (new hires, newly enrolled students) get prompt training as part of onboarding, so there's no gap in awareness. A great practice is to maintain a library of micro-learning modules or short videos that can be sent out periodically ("Secure Passwords 101" this month, "How to spot a phishing link" next month, etc.). This continuous education mindset ensures cybersecurity stays top-of-mind and knowledge levels improve steadily.
- **Monitor, Audit, and Feedback Loops:** Establish processes to continually **monitor the effectiveness** of your security culture. This includes technical monitoring (like detecting how many malware or phishing attempts were blocked and if any got through) as well as cultural monitoring (like checking if policies are being followed on the ground). Conduct periodic audits or check-ups: for example, do random "spot checks" to see if schools are keeping their student data cabinets locked and computers logged off when not in use – physical security habits are part of cyber awareness too. Use the metrics you gathered (as discussed earlier) to identify where things might be slipping. If you notice, for instance, an uptick in incidents or a slide in training completion, investigate why and address it. **Solicit feedback** from users as well: maybe staff say the phishing simulations are too predictable now, so attackers would just use a trickier method – that's an opportunity to up your game. Or maybe teachers find the training modules too long – that feedback could drive you to break them into shorter segments. Creating a feedback loop signals that the board is not just preaching but also listening and improving, which helps keep people engaged.
- **Recognize and Reward Good Practices:** Positive reinforcement goes a long way in culture building. Recognize schools or individuals demonstrating excellent cybersecurity practices. This could be as simple as an appreciation email from the Director to a school that had zero phishing clicks in a quarter, or a shout-out to the IT team for successfully implementing a new safety measure. Some boards have given fun titles like "Cyber Champion of the Month" to staff who actively promote security. For students, you might have competitions or

badges for completing digital citizenship activities. Publicize success stories: *"This week, a teacher at School X spotted and reported a phishing attempt — preventing any breach. Great catch!"* This not only rewards the vigilant, but also shows others the real impact of awareness. It builds a sense of pride that *we as a community are getting more cyber-smart*. Over time, this positive culture can become self-reinforcing, where people take initiative because they feel it's valued.

- **Stay Informed and Adaptable:** The cybersecurity field can change quickly with new threats (witness how quickly ransomware grew, or how AI tools are now being used in scams). **Ensure someone in the board (or a team)** is tasked with staying up-to-date on threat intelligence and industry best practices [5]. This could be the CIO, the IT security lead, or involvement in information-sharing groups like the provincial Cyber Security Division's education forums. When new risks emerge, communicate them promptly to staff and adjust guidance accordingly. For example, if there's news about a new malware targeting education institutions, send an advisory to all staff on what to watch out for. Being agile and proactive keeps the culture from stagnating. It also demonstrates leadership's continued commitment — that this isn't a one-time project but a living, adaptive program.
- **Strengthen Collaboration and Knowledge Sharing:** Encourage an environment where schools learn from each other and from external sources. The board can organize an annual cybersecurity summit or workshop day for school tech reps to exchange ideas and success stories. Participate in sector-wide initiatives – Ontario has a strong collaborative approach (boards share resources via ECNO, and the Ministry coordinates campaigns [10]). Leverage that network: attend webinars, read the case studies of what other boards did after an incident. Share your board's experiences too, which contributes to the collective improvement. As Patricia Kosseim advocated, **boards should collaborate more often to share best practices** [1] – it helps everyone improve and keeps each board from working in isolation on the same problems. The more cybersecurity is treated as a community effort, the better prepared all schools will be.
- **Maintain Incident Readiness:** Continuously refine your incident response capabilities. Run a full simulation drill at least once a year (maybe every semester) that involves not just IT, but also communications, school management, and even student/parent communication plans. Each drill will reveal new things to improve – take those lessons and update your playbooks. Keep contact lists (for your incident response team, emergency vendors, legal counsel, etc.) updated. Because when an incident does strike in the future, a well-prepared team that has practiced will handle it far more smoothly, mitigating damage. A quick, effective incident response will in turn reinforce the

culture ("we were hit, but we managed it well because we were prepared"). It validates the efforts put into awareness and readiness.

- **Integrate Cybersecurity into the Board's Identity:** Finally, aim to **make cybersecurity part of the organizational DNA**. Include a security/privacy impact assessment in planning any new initiative (just like one might consider budgets or educational outcomes, consider cybersecurity impact). In strategic documents or annual reports, mention the board's commitment to cybersecurity alongside other values. When onboarding new principals or department heads, brief them on their role in fostering this culture. Essentially, institutionalize it so deeply that it survives leadership changes and becomes a permanent priority. This helps maintain momentum over the years. We are already seeing this in some policy guidance – for example, the Ministry's PPM guidelines explicitly tell boards to create a culture of cybersecurity and privacy awareness across all levels [4]. Down the line, maintaining a cyber aware culture might even become an expectation in board evaluations or Ministry assessments.

By following these best practices, a school board can ensure that its cyber aware culture not only **takes root, but continues to flourish**. The cybersecurity landscape will always pose challenges, but a well-cultivated culture becomes a powerful, adaptive defense mechanism. It turns your people from potential targets into the first line of defense. As we empower our educators and students with knowledge and tools, we create a safer digital environment for learning.

Conclusion

In today's digital age, **creating a cyber aware culture is as fundamental to a school board's success as fostering a positive learning culture**. Cybersecurity can no longer be siloed or left to a few IT specialists; it must be a shared value ingrained in how the board operates daily. For Ontario's publicly funded school boards, this cultural shift is not just ideal – it is imperative. Cyber threats are real and growing for the education sector, but by proactively building awareness and resilience, we can turn those threats into manageable risks.

The *good news* is that Ontario's education community is rising to the challenge. With support from organizations like ECNO and initiatives from the Ministry of Education [10], boards have more resources than ever to educate and protect their communities. Many boards have already made strides by partnering together, such as the 66 boards collaborating on ECNO's security services [8]. This collaborative spirit, combined with strong local leadership, can ensure that every board – large or small, urban or rural, English or French – can elevate its security posture.

For senior board leaders – Directors, Superintendents, CIOs – **the call to action is clear**. By championing a cyber aware culture:

- You *empower your staff and students* to navigate the digital world safely.
- You *protect the mission of education* from avoidable interruptions.
- You *safeguard the trust* that families place in our school systems.
- You *ensure compliance* with the evolving regulatory landscape.
- And you *enable the exciting potential of technology* in education by managing its risks responsibly.

As we have seen, building this culture involves investment and effort across policies, training, and community engagement. It may seem daunting, but step by step, the change is achievable – and numerous successes and best practices are available to guide the way. The payoff is a school board where cybersecurity becomes second nature, much like locking the doors or practicing fire drills. In such an environment, everyone can focus more on teaching and learning, because the foundation of trust and safety in our digital systems has been laid.

In conclusion, a cyber aware culture is not just an IT initiative – it's an educational imperative and a leadership opportunity. By instilling cyber awareness as a core value, we prepare our schools to securely harness technology's benefits while keeping threats at bay. Let's work together to foster a generation of cyber-aware educators, students, and communities, so that Ontario's K-12 education remains not only innovative and effective, but also safe and secure for all. [41]